# User's Manual

**Version: 2.2**

# AWOS2400050

# High Power Integrated Outdoor CPE 2.4GHz

**Trademarks**

Copyright @2007

All trademarks belong to their respective proprietors.

All rights reserved. No part of this document may be reproduced in any form or by any means without written permission from the product manufacturer.

Changes are periodically made to the information in this document. They will be incorporated in subsequent editions. The product manufacturer may take improvement and/or changes in the product described in this document at any time

**Copyright Statement**

**THIS DOCUMENT CONTAINS OF PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THIS COMPANY. AND NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRICAL OR MECHANICAL, BY PHOTOCOPYING, RECORDING, OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF THIS COMPANY.**

# Declaration of Conformity CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

**Countries of Operation and Conditions of Use in the European Community**

This device is intends to be operated in all countries of the European Community. Requirement is for indoors or outdoors operation, license requirements and allowed channels of operation apply in some countries.

**Solwise Ltd.**

17 Priory Tec Park
Saxon Way
Hessle
Hull HU13 9PB
UK

Tel: 0845 458 4558 (local rate)
Fax: 0845 458 4559
Support Tel: 0845 458 5819
Email sales@solwise.co.uk
Http www.solwise.co.uk

## Contents


1. FEATURES OVERVIEW ..... 1
2. FIRMWARE INSTALLATION ..... 3
   2.1 FIRMWARE INSTALLATION VIA WEB INTERFACE ..... 3
   2.2 FIRMWARE INSTALLATION BY TFTP ..... 4
3. SECURITY INFORMATION ..... 6
4. CONFIGURATION ..... 7
   4.1 Status ..... 7
      4.1.1 Status ..... 7
      4.1.2 Active Clients ..... 7
      4.1.3 DHCP Clients ..... 7
   4.2 Wireless ..... 7
      4.2.1 Basic ..... 7
      4.2.2 Disable Wireless Interface ..... 7
      4.2.3 Name ..... 7
      4.2.4 Frequency/Modulation ..... 7
      4.2.5 Mode ..... 7
      4.2.6 Network Type ..... 8
      4.2.7 SSID ..... 8
      4.2.8 SSID Universal Repeater ..... 8
      4.2.9 Region Domain ..... 8
      4.2.10 Channel Number ..... 8
   4.3 Advanced ..... 9
      4.3.1 Authentication Type ..... 9
      4.3.2 ACK Timeout ..... 9
      4.3.3 Fragmentation Threshold ..... 9
      4.3.4 RTS Threshold ..... 9
      4.3.5 Beacon Interval ..... 9
      4.3.6 Data Rate ..... 9
      4.3.7 DTIM Period ..... 9
      4.3.8 Preamble Type ..... 9
      4.3.9 Block Relay ..... 10
      4.3.10 Hide SSID ..... 10
      4.3.11 IAPP ..... 10
      4.3.12 802.11g Protection ..... 10
      4.3.13 Power ..... 10
   4.4 Security ..... 10
   4.5 Access Control ..... 10
   4.6 Site Survey ..... 11

4.7 WDS....11
4.8 Signal Meter....11
5. TCP/IP....12
5.1 Operation Mode....12
5.2 Basic....12
5.2.1 Bridge....12
5.2.2 Gateway - *this mode is irrelavent since the WAN port is not used on the AWOS outdoor product* 13
5.2.3 Gateway - Wireless and LANs Bridge - *this mode is irrelavent since the WAN port is not used on the AWOS outdoor product*....14
5.2.4 Wireless ISP....14
5.2.5 Wireless ISP - LANs Bridge....15
5.3 Advanced....16
5.3.1 NAT....16
5.3.2 HTTP Port....16
5.3.3 Remote Management....16
5.3.4 SSH Server / SSH Server Port....17
5.3.5 Block P2P....17
5.3.6 Block NETBIOS....17
5.4 IP Alias....17
5.5 Static Route....17
6. Firewall....18
6.1 Layer7 Filter....18
6.1.1 Source....18
6.1.2 Destination....18
6.1.3 Protocol....18
6.2 Port Filter....18
6.3 Port Forwarding....19
6.4 IP Filter....19
6.5 MAC Filter....19
6.6 DMZ Zone....19
7. Bandwidth Control....20
7.1 Interface Bandwidth....20
7.2 IP/MAC Bandwidth....20
7.2.1 IP/IP Range/MAC Bandwidth Control....20
7.2.2 Add Layer7 Rules....20
8. Others....21
8.1 Personal script....21
8.2 Ethers/DHCP script....21
8.3 Proxy ARP script....21

8.4 Reboot ..... 21
8.5 System Commands ..... 21
8.6 Date/Time ..... 21
8.7 Upgrade Firmware ..... 21
8.8 Save Configurations ..... 21
8.9 License ..... 21
8.10 Password ..... 22
8.11 Watchdog ..... 22
8.12 Dynamic DNS ..... 22
8.13 Apply Configurations ..... 22

# 1. FEATURES OVERVIEW

- 5 operational modes: Bridge, Gateway, Gateway - Wireless and LAN Bridge, Wireless ISP, and Wireless ISP - LAN Bridge
- Up to 254 programmable IPs/MACs for Bandwidth Control
- Bandwidth control by IP, IP Range, or MAC, integrated with Layer 7 (protocol identification) P2P control
- Bandwidth control in bridge mode
- Support to ebtables (bridging firewall)
- Graphic signal level meter, with real-time RSSI
- Power control up to 250 mW (11b only)
- Universal Repeater with 'meshing' using OLSR (see http://www.olsr.org)
- Configuration method: Save then Apply
- IP Aliasing, up to 254 IPs
- Layer 7 Filter (block services using application layer pattern matching to identify the protocol)
- Option to change WEB server port
- Option to enable/disable SSH Server
- Option to change the SSH server port
- Option to block P2P protocols (eDonkey, Ares, Fasttrack, Gnutella, etc.)
- Option to block NetBIOS (Windows network traffic)
- Web interface configuration and management
- SSH Client
- ACK timeout
- MAC cloning (for one machine)
- Personal script editing via WEB or SSH
- Proxy ARP script editing via WEB or SSH
- Ethers/DHCP script editing via WEB or SSH
- Region Domain selection (11 or 14 channels)
- tcpdump via SSH
- per-IP watchdog
- Hide SSID
- WEP, WPA, WPA2, 802.1x and Radius security
- Auto Discovery Tool
- Dynamic DNS Support
- Client, AP, AP+WDS, WDS and Universal Repeater
- Spanning Tree Protocol
- IAPP (Inter-Access Point Protocol)
- 802.11g Protection mode
- Site Survey
- DHCP Server

- DHCP Client
- PPPoE Client
- MAC, IP, port filtering
- DMZ Host

## 2. FIRMWARE INSTALLATION

**Requirements:**

- Realtek RTL 8186 based equipment
- Minimum 16MB RAM and 2MB Flash

**Notes about the Tx Power Control:**

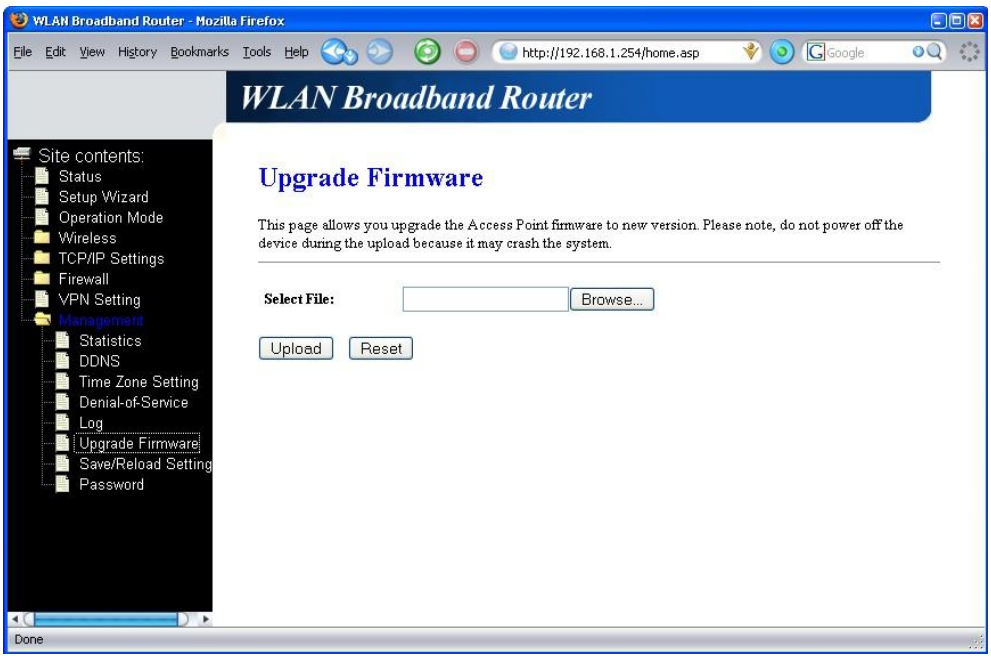
The Tx power control setting only applies to 802.11b mode.

The Router has the power limited to 250mw by HARDWARE.

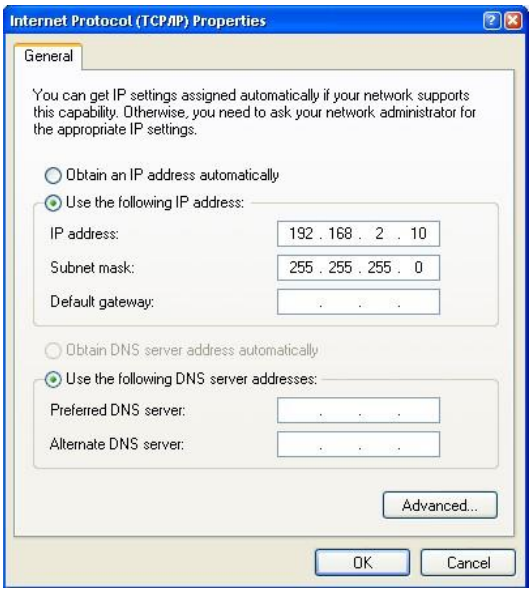
THE HIGHEST POWER MAY NOT BE THE IDEAL SETTING FOR ALL APPLICATIONS. TEST DIFFERENT SETTINGS TO FIND THE BEST ADJUSTMENT FOR YOUR SPECIFIC APPLICATION.

### 2.1 FIRMWARE INSTALLATION VIA WEB INTERFACE

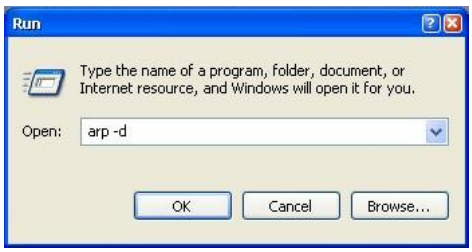
1. Save the firmware file (ROUTERPRO_vx_x_xmodx.bin) and the license file (.dat) in your local disk.
2. Follow your original router instructions to connect to the device using the web interface and look for the "Upgrade Firmware" or "Update Firmware" option.



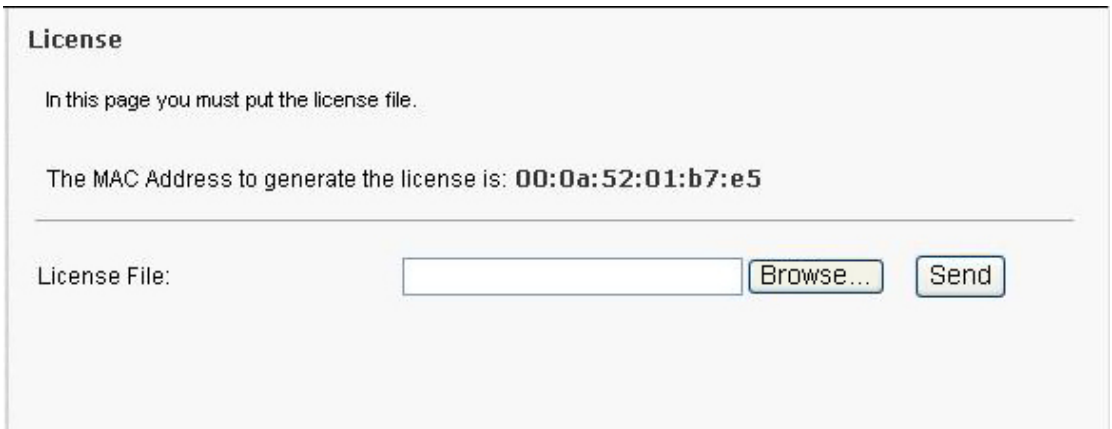

3. Browse for the " Router PRO - xxx - Vyyy.bin", and upload it (xxx and yyy indicate the customization and version)
4. Wait for the update process to complete. It may take about one minute after the file is uploaded
5. After the update process finishes, the device IP will be reset to 192.168.2.1. You will need to set your PC's address to an IP in the same subnet, for example, 192.168.2.10 in the Windows Control Panel -> Network Connections -> Local Area Connection -> Properties -> Internet Protocol (TCP/IP): *(take note of your original configuration so you can restore it later)*


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 2 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Access the router by typing the address http://192.168.2.1 in your browser. If you cannot access the device, try cleaning the ARP table, by running the command "arp -d" with Start, Run, then try again:


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: arp -d
OK
Cancel
Browse...

7. Once in the web interface of the new firmware SQ ROUTER PRO, select to the License menu option, and check if the MAC address matches the name of the .dat file with the license to be uploaded.
8. Select the .dat license file and upload it. Wait for 2 minutes for the process to complete (the router will reboot). Your device will then be ready to be configured.

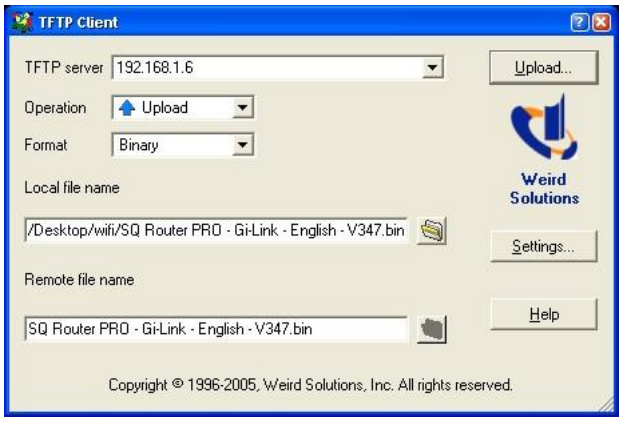



## 2.2 FIRMWARE INSTALLATION BY TFTP

The TFTP installation method can be used if it is not possible to access the web interface, or if it is not possible to upload the firmware through the web interface.

1. If you don't have a TFTP client program, download and install one. There are several free options available on the web. The procedure below uses the free TFTP client available at:
   http://www.weirdsolutions.com/weirdSolutions/files/products/desktopSoftware/desktopTftpClient/tftpc_free.exe
2. Configure your PC's IP address to 192.168.1.10
3. Connect the AWOS to the network using one of the 4 LAN ports

4. Turn the device off, hold the reset button pressed, and turn the device back on. Wait for 5 seconds before releasing the reset button.
5. The AWOS will be in TFTP mode, with IP 192.168.1.6, awaiting for the firmware upload
6. Run the TFTP Client, with the setting: TFTP server = 192.168.1.6, Operation = Upload, and Format = Binary.
7. Select the .bin firmware file for upload, and click "Upload":




8. After the upload finishes, wait for 1 minute for the device to reboot, and access it again from the web interface (remember that with the SQ Router Pro firmware, the default IP address will be 192.168.2.1, so you will need to change your PC IP address to 192.168.2.10 to access it)
9. Once in the web interface, access the License menu option and upload the license .dat file.

## 3. SECURITY INFORMATION

### Web interface password

The access to the web configuration interface has no username/password by default. Make sure you set up a username and password to prevent unauthorized access to this interface.

### root password

The ssh access is enabled by default, and the default root password is **admin**. If you are going to keep the ssh access enabled, make sure to change the root password to prevent unauthorized access.

To change the root password, access the device through ssh and log in as root. Use the **passwd** command to change the password, then the **save** command to store the change in the flash memory (if you skip the save command, the password will revert to the previous one on the next reboot).

# 4. CONFIGURATION

The configuration is done through a friendly and dynamic web interface. The default web address is 192.168.2.1. To enter configuration enter the address 192.168.2.1 on your browser address bar and press enter.

Configuration uses a "Save then Apply" method, so it is possible to set all the options first, then apply them once. Remember that the settings will only be used after you apply them with the "**Apply Configurations**" menu option.

## 4.1 Status

### 4.1.1 Status

Shows the device's main configuration settings

### 4.1.2 Active Clients

Shows information about the wireless clients connected to the device, in Client or AP Mode.

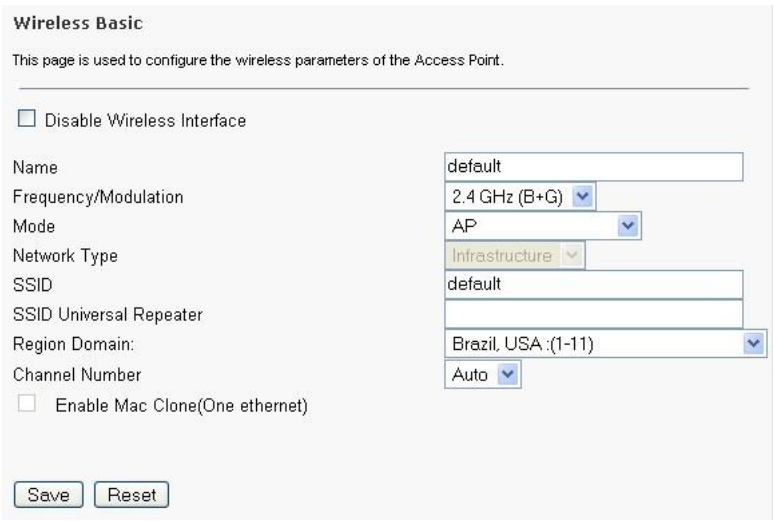
### 4.1.3 DHCP Clients

Shows IP, MAC, and Lease Remaining Time for the DHCP clients connected to the Access Point.

## 4.2 Wireless

### 4.2.1 Basic

Basic Access Point settings configuration. It is also possible to disable/enable the wireless interface, and to enable the Clone MAC function.




### 4.2.2 Disable Wireless Interface

Turns the Wireless Interface on/off. Turning off the Wireless Interface can be useful if you just want to use the device as a Ethernet Router, with the filtering and bandwidth control features.

### 4.2.3 Name

Device name for identification.

### 4.2.4 Frequency/Modulation

Selects the frequency and modulation standard to use. For the AWOS, the only frequency available is 2.4GHz. You can select B, G, or B+G for 802.11b, 802.11g or 802.11b+802.11g.

### 4.2.5 Mode

The following operational modes are available:

**AP:** (Access Point) The device will be the main Wireless Access Point in the wireless network, and wireless clients will connect to it. The wireless clients may be other AWOSs in Client mode, or computers with compatible wireless network adapters.

**Client:** The device will connect to another device in AP mode, if configured with the same SSID. Other devices in Client mode and the Ad-Hoc option enabled can also be connected.

**WDS:** (Wireless Distribution System) This system allows the interconnection of multiple Access Points through the wireless link, expanding the coverage of the wireless network without the need of a wired connection between them. To use WDS, there should be other device(s) operating in WDS or AP+WDS mode within the wireless reach, and the MAC of each device has to be added to the other device's WDS list, in the Wireless - WDS menu. The WDS devices will operate as transparent bridges.

**AP+WDS:** The device will operate both as an Access Point, and as a WDS node for coverage extension.

**Universal Repeater:** Also a way of extending the wireless coverage, simpler than the WDS method. The device will connect and repeat the signals from another device in AP mode. Both devices must be set to the same channel and SSID. The device will operate as a transparent bridge. Enabling this mode also turns on meshing ability using OLSR. With OLSR functions the IP routing is automatically adjusted to give the most cost effective route for IP traffic. This gives route redundancy and also ensures that traffic always takes the best route through the system. It also means that when a client moves from one cell (one AP router) to the other then the AP's automatically change the route path to ensure the lowest cost.

#### 4.2.6 Network Type

Selectable in Client Mode only; the following types are available:

**Infrastructure:** Device will connect to an Access Point in the network

**Ad-Hoc:** Device will connect to other devices in Ad-Hoc mode.

#### 4.2.7 SSID

Service Set Identifier of the wireless network, up to 32 characters. If in Client Mode, should be set to the SSID of the Access Point to which the device will be connected. If in AP mode, this will be the SSID used by this Access Point.

#### 4.2.8 SSID Universal Repeater

In the Universal Repeater mode, this defines the SSID used by clients to connect to this Access Point.

#### 4.2.9 Region Domain

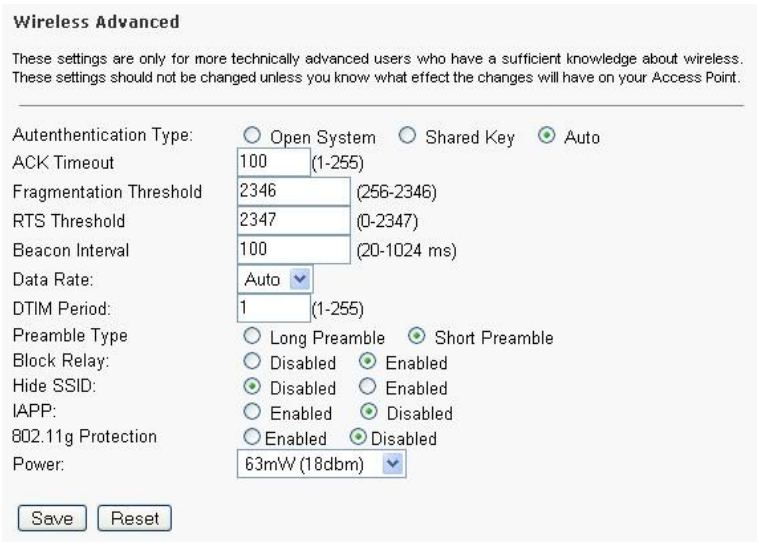
Defines the set of available channels, according to the local regulations for each region.

#### 4.2.10 Channel Number

Wireless channel to be used by the device. The range of available channels is dependent of the Region Domain setting. If set to Auto, the device will automatically select the channel with less noise to minimize interference.

## 4.3 Advanced

Advanced configuration options for the wireless operation.


Wireless Advanced
These settings are only for more technically advanced users who have a sufficient knowledge about wireless. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Autenthentication Type: Open System Shared Key Auto
ACK Timeout 100 (1-255)
Fragmentation Threshold 2346 (256-2346)
RTS Threshold 2347 (0-2347)
Beacon Interval 100 (20-1024 ms)
Data Rate: Auto
DTIM Period: 1 (1-255)
Preamble Type Long Preamble Short Preamble
Block Relay: Disabled Enabled
Hide SSID: Disabled Enabled
IAPP: Enabled Disabled
802.11g Protection Enabled Disabled
Power: 63mW (18dbm)
Save
Reset

### 4.3.1 Authentication Type

Selects the Wireless network authentication type.

### 4.3.2 ACK Timeout

Sets the maximum time the AP will wait for a remote wireless device to acknowledge a packet, before retransmitting it.

### 4.3.3 Fragmentation Threshold

Frames larger than this setting will be divided and sent through the wireless network in smaller fragments. If there is no interference, the ideal value is the maximum setting. For areas with interference, try smaller sizes.

### 4.3.4 RTS Threshold

If a frame is larger than this setting, devices are required to exchange a RTS (Request To Send)/CTS (Clear To Send) pair before sending it. Lower values can enhance performance if there are many wireless clients in the network, or if clients are far from each other (so they can see the AP, but not other clients). The default 2347 value means RTS is disabled.

### 4.3.5 Beacon Interval

Time between beacon transmissions.

### 4.3.6 Data Rate

Sets the wireless network data rate. Leaving this in Automatic will allow the AP to automatically adjust the data rate according to the wireless link conditions.

### 4.3.7 DTIM Period

DTIM is the Delivery Traffic Indication Message. This setting defines the interval, in number of beacons, for the inclusion of the DTIM in the AP beacon.

### 4.3.8 Preamble Type

Selects between long and short preamble. The Short Preamble allows better throughput. Long preamble is better in noisy environments, and for compatibility with older devices, not supporting the short type.

4.3.9 Block Relay

Prevents that two wireless clients can communicate to each other directly through the access point.

4.3.10 Hide SSID

Prevents the SSID to be sent in the AP broadcast messages, so it cannot be found by AP scanners.

4.3.11 IAPP

Enables the Inter Access Point Protocol

4.3.12 802.11g Protection

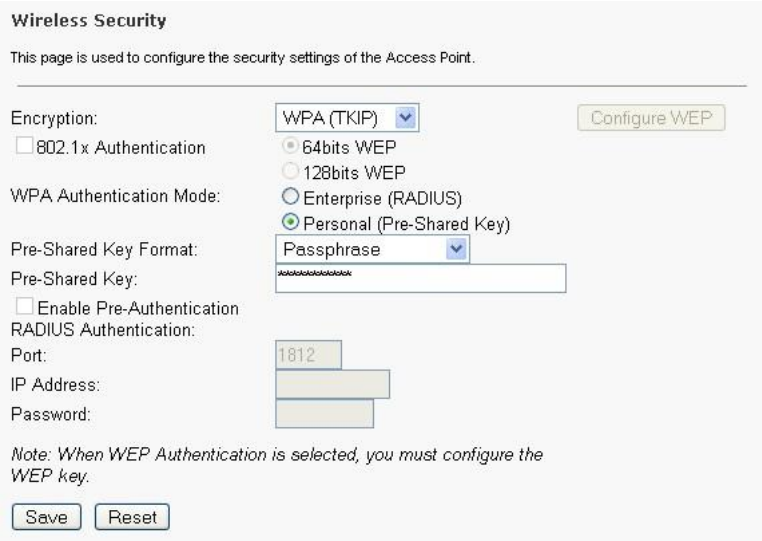
In a mixed 802.11b and 802.11g environment, prevents interference between both systems.

4.3.13 Power

Adjusts the transmission power of the device. Only use higher values if necessary for the application, according to the distance.

## 4.4 Security

Authentication and security setup. Sets the encryption type, and the authentication options.



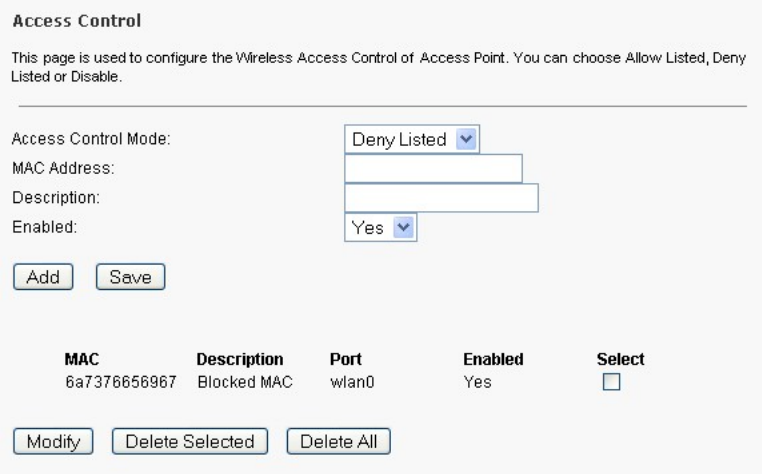

## 4.5 Access Control

Allows the set up a list of MAC addresses for access control. The Access Control Mode can be set to:

**Disabled:** No MAC address access control is enforced.

**Deny Listed:** The devices with MAC addresses listed in the table are denied access to the wireless network. All other devices are allowed.

**Allow Listed:** The devices with MAC addresses listed in the table are allowed access to the wireless network. All other devices are denied.




The MAC Access Control can also be set through the Personal Script menu option. In this case, the access control only needs to be enabled in this page, and the MACs configured in the Personal Script.

## 4.6 Site Survey

Shows the available wireless networks, and allows the connection to one of them (in Client Mode).

## 4.7 WDS

Edits the WDS MAC table, which lists the other devices in the Wireless Distribution System. The device has to be set to WDS or AP+WDS mode.

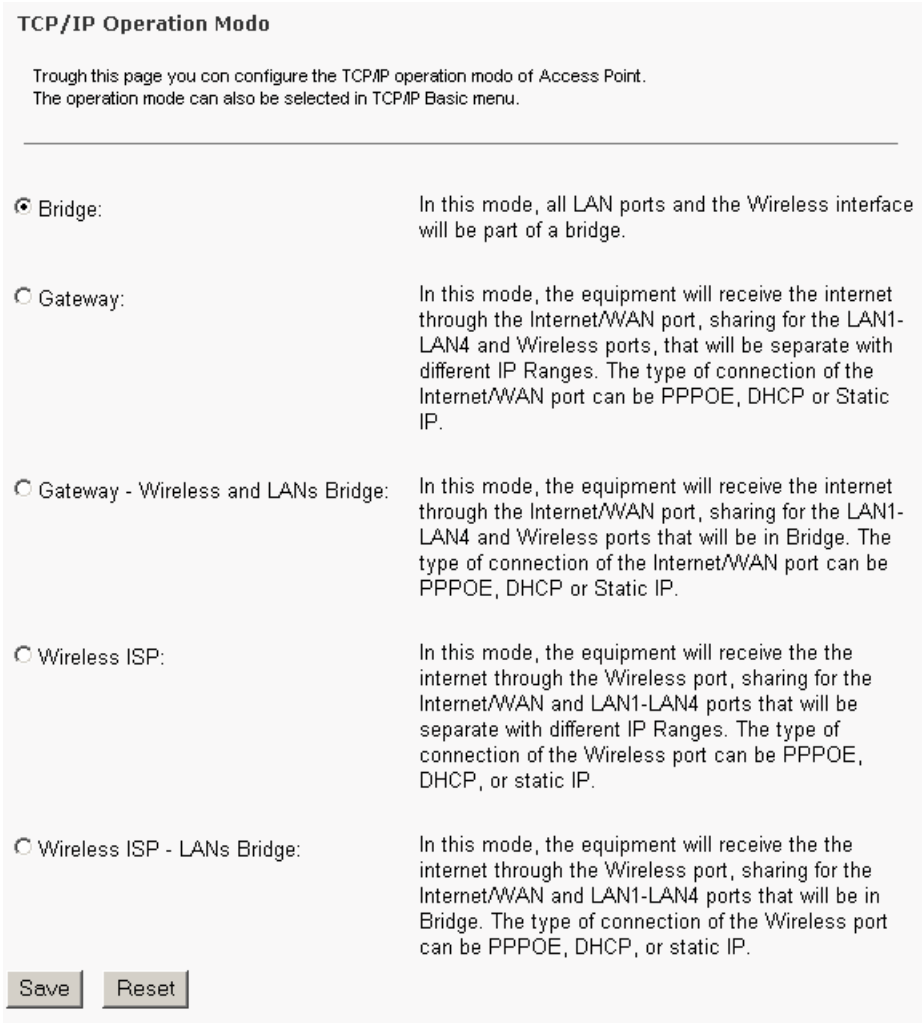
## 4.8 Signal Meter

Shows a signal meter bar, with the device's received signal strength indication (RSSI).

# 5. TCP/IP

## 5.1 Operation Mode

Sets the TCP/IP operation mode – this mode can also be set in the TCP/IP Basic setup

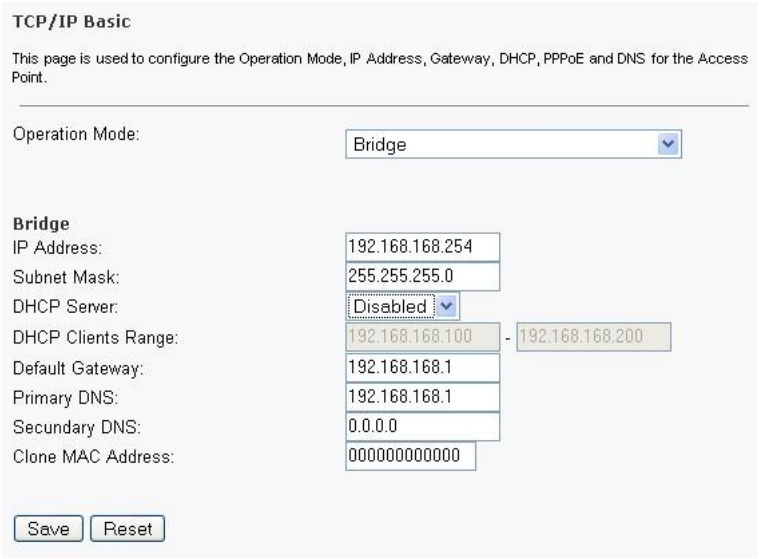

TCP/IP Operation Modo
Trough this page you con configure the TCP/IP operation modo of Access Point.
The operation mode can also be selected in TCP/IP Basic menu.
Bridge:
In this mode, all LAN ports and the Wireless interface will be part of a bridge.
Gateway:
In this mode, the equipment will receive the internet through the Internet/WAN port, sharing for the LAN1-LAN4 and Wireless ports, that will be separate with different IP Ranges. The type of connection of the Internet/WAN port can be PPPOE, DHCP or Static IP.
Gateway - Wireless and LANs Bridge:
In this mode, the equipment will receive the internet through the Internet/WAN port, sharing for the LAN1-LAN4 and Wireless ports that will be in Bridge. The type of connection of the Internet/WAN port can be PPPOE, DHCP or Static IP.
Wireless ISP:
In this mode, the equipment will receive the the internet through the Wireless port, sharing for the Internet/WAN and LAN1-LAN4 ports that will be separate with different IP Ranges. The type of connection of the Wireless port can be PPPOE, DHCP, or static IP.
Wireless ISP - LANs Bridge:
In this mode, the equipment will receive the the internet through the Wireless port, sharing for the Internet/WAN and LAN1-LAN4 ports that will be in Bridge. The type of connection of the Wireless port can be PPPOE, DHCP, or static IP.
Save
Reset

## 5.2 Basic

Configuration settings for the TCP/IP operation. Each mode of operation has a different settings screen, described below.

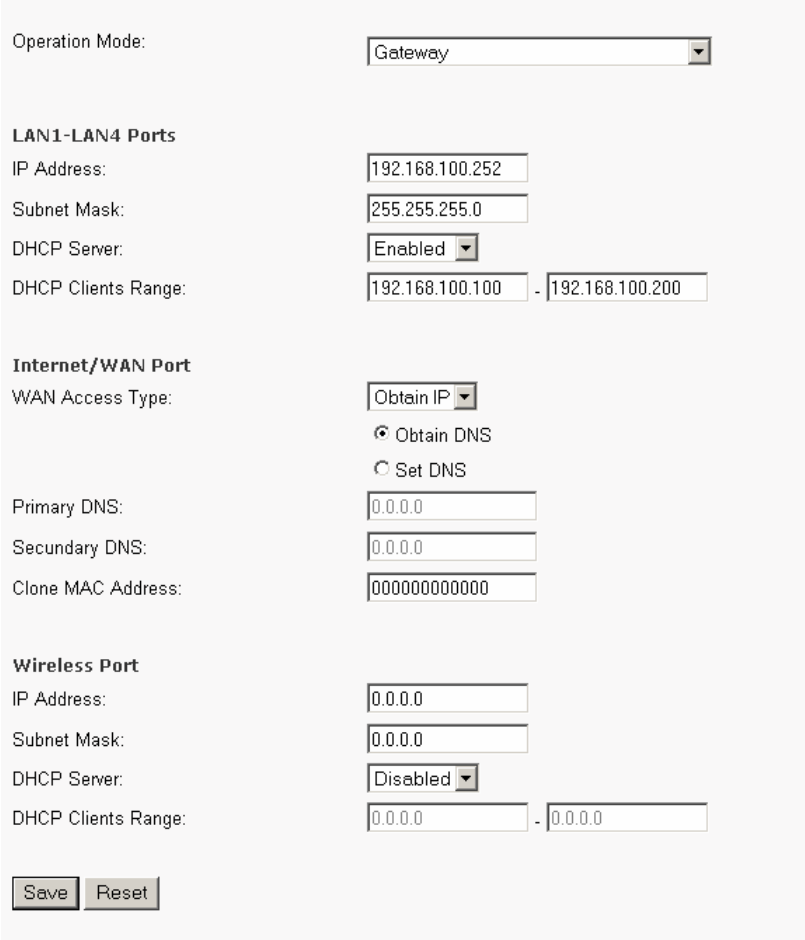
### 5.2.1 Bridge

In this mode, the device operates as a transparent bridge, interconnecting the wireless network and all the ethernet (LAN) ports. The firewall-related functions and NAT are not available in this mode.




5.2.2 Gateway - *this mode is irrelavent since the WAN port is not used on the AWOS outdoor product*

In this mode, the device connects to the ISP through the WAN port, and shares this connection with the LAN and Wireless Network. The LAN ports will belong to one IP subnetwork, and the Wireless interface to another one.



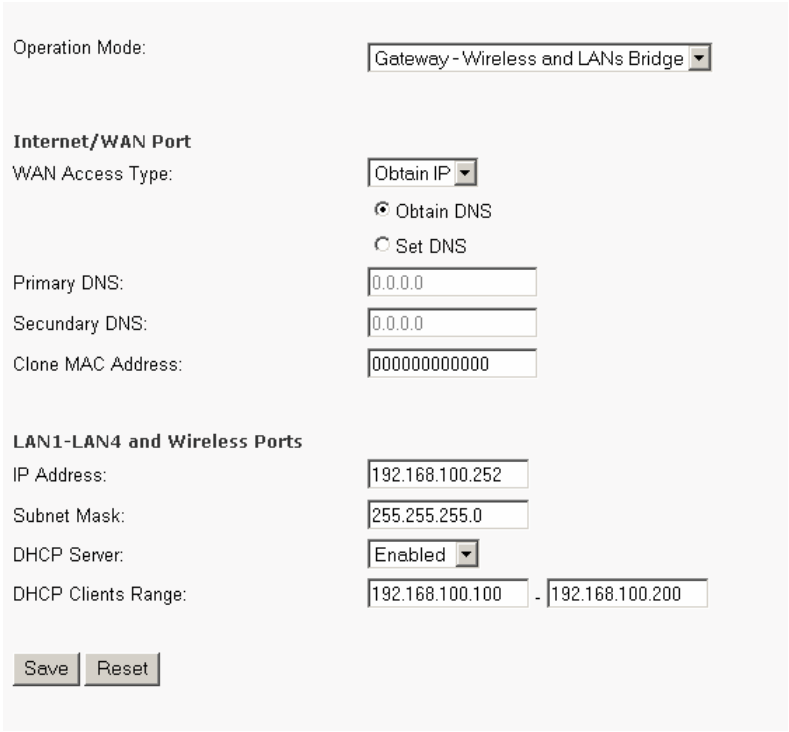

**LAN1-LAN4 Ports:** Sets the IP and Subnet Mask for the LAN1-4 ports. A DHCP server can be enabled and configured for this subnetwork.

**Internet/WAN Port:** Configures the WAN Access Type - Obtain IP (DHCP), Static IP, or PPPoE. Also sets the MAC address which the WAN port will assume for the ISP (MAC Cloning).

**Wireless Port:** Sets the IP and Subnet Mask for the Wireless Interface. A DHCP server can be enabled and configured for this subnetwork.

5.2.3 Gateway - Wireless and LANs Bridge - *this mode is irrelavent since the WAN port is not used on the AWOS outdoor product*

In this mode, the device connects to the ISP through the WAN port, and shares this connection with the LAN and Wireless Network. The LAN ports and Wireless interface will belong to the same IP subnetwork (transparent bridge).

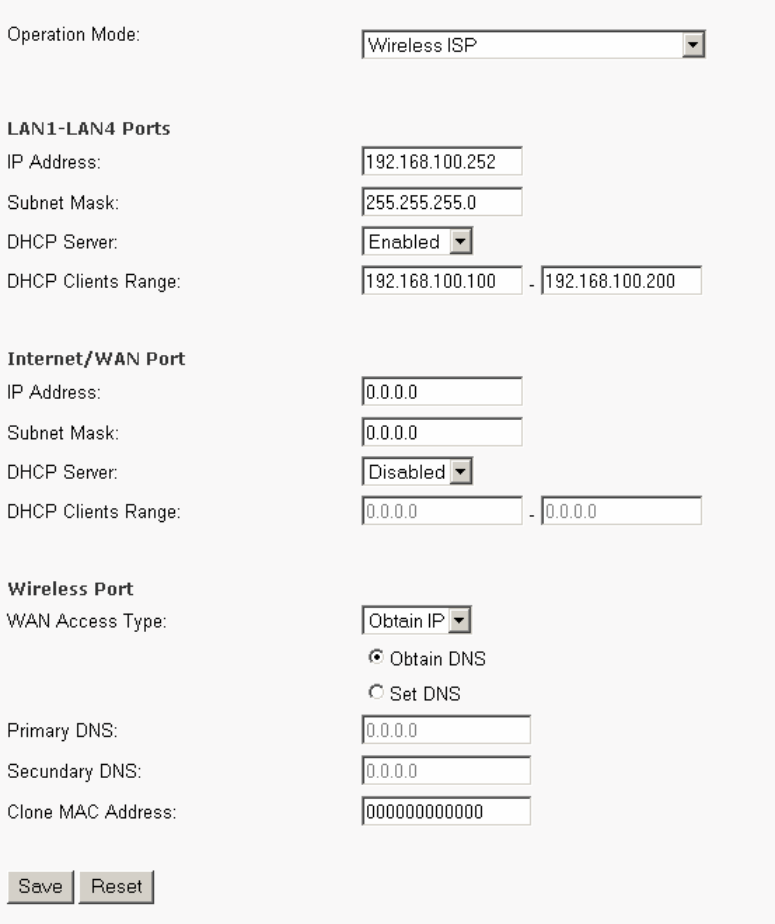



**Internet/WAN Port:** Configures the WAN Access Type - Obtain IP (DHCP), Static IP, or PPPoE. Also sets the MAC address which the WAN port will assume for the ISP (MAC Cloning).

**LAN1-LAN4 and Wireless Port:** Sets the IP and Subnet Mask for the LAN and Wireless interfaces. A DHCP server can be enabled and configured for this subnetwork.

5.2.4 Wireless ISP

In this mode, the device connects to the ISP through the Wireless interface, and shares this connection with the LAN and WAN ports. The LAN1-LAN4 ports will belong to one IP subnetwork, and the WAN port will belong to another one (Note the WAN port is not used on the outdoor AWOS product).



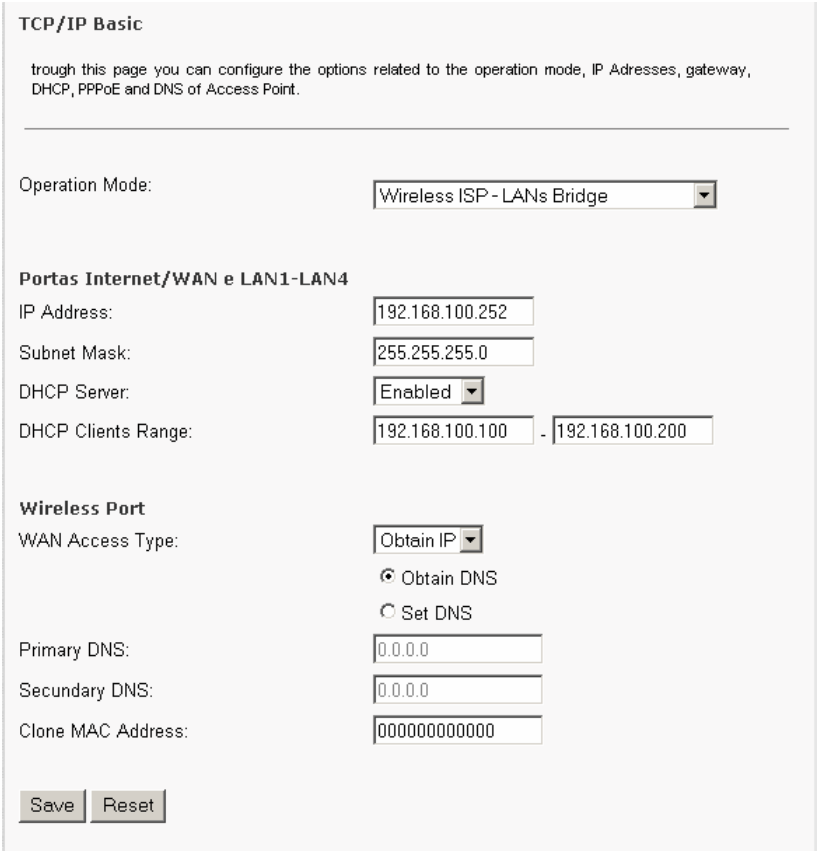

**LAN1-LAN4 Ports:** Sets the IP and Subnet Mask for the LAN1-4 ports. A DHCP server can be enabled and configured for this subnetwork.

**Internet/WAN Port:** Sets the IP and Subnet Mask for the WAN port. A DHCP server can be enabled and configured for this subnetwork. Note the WAN port is not used on the outdoor AWOS product.

**Wireless Port:** Configures the Wireless ISP Access Type - Obtain IP (DHCP), Static IP, or PPPoE. Also sets the MAC address which the Wireless interface will assume for the ISP (MAC Cloning).

### 5.2.5 Wireless ISP - LANs Bridge

In this mode the device connects to the ISP through the wireless interface and shares this connection with the LAN and WAN ports. The LAN1-LAN4 and WAN ports all belong to the same IP subnet (transparent bridge). Note the WAN port is not used on the outdoor AWOS product.

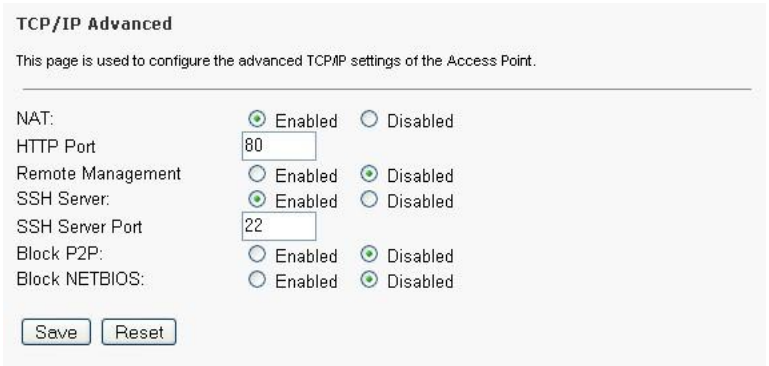



**Internet/WAN and LAN1-LAN4 Ports:** Sets the IP and Subnet Mask for the WAN and LAN1-4 ports. A DHCP server can be enabled and configured for this subnetwork.

**Wireless Port:** Configures the Wireless ISP Access Type - Obtain IP (DHCP), Static IP, or PPPoE. Also sets the MAC address which the Wireless interface will assume for the ISP (MAC Cloning).

## 5.3 Advanced

Configures advanced TCP/IP options.




### 5.3.1 NAT

Enables the Network Address Translation, masquerading the client IPs as one single IP to the ISP.

### 5.3.2 HTTP Port

Configures the TCP port for the internal web server for the web configuration interface.

### 5.3.3 Remote Management

Configures the TCP port for the internal web server for the web configuration interface.

5.3.4 SSH Server / SSH Server Port

Enables the SSH server, and sets the TCP port for the server to listen to.

5.3.5 Block P2P

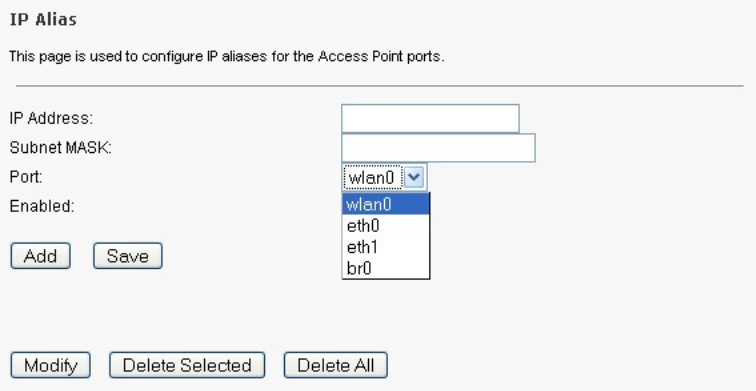
Enables the P2P protocols blocking.

5.3.6 Block NETBIOS

Blocks the NETBIOS protocol (Windows/SMB networking).

## 5.4 IP Alias

Allows the setting of additional IP addresses (IP Aliasing) for each of the interfaces.




The interfaces are:

**wlan0:** Wireless interface
**eth0:** LAN Interface
**eth1:** WAN Interface Note the WAN port is not used on the outdoor AWOS product.
**br0:** Bridge interface (transparently bridged interfaces are unified as br0)

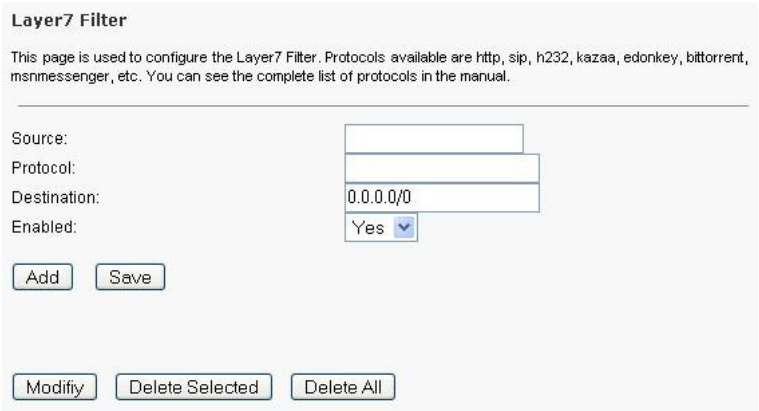
## 5.5 Static Route

Manipulates the routing table for the device.

# 6. Firewall

## 6.1 Layer7 Filter

Allows blocking traffic using protocol identification at the application layer (independently from the TCP port). For a packet to be blocked, its Source, Destination, and Protocol must match the filter rule.




### 6.1.1 Source

Source IP of the packet, in the format <IP>/<number of bits of the subnet mask>. 0.0.0.0/0 means any IP.

### 6.1.2 Destination

Destination IP of the packet, in the format <IP>/<number of bits of the subnet mask>. 0.0.0.0/0 means any IP.

### 6.1.3 Protocol

Protocol to match the traffic signature. The currently supported protocol names are listed below:

| | | | | |
|---|---|---|---|---|
| **100bao** | **gopher** | **poco** | **unknown** | **smb** |
| **aim** | **h323** | **pop3** | **uucp** | **smtp** |
| **aimwebcontent** | **halflife2-deathmatch** | **pressplay** | **validcertssl** | **snmp** |
| **applejuice** | **hddtemp** | **qq** | **ventrilo** | **socks** |
| **ares** | **hotline** | **quake1** | **vnc** | **soribada** |
| **battlefield1942** | **http** | **quake-halflife** | **whois** | **soulseek** |
| **battlefield2** | **http-rtsp** | **rdp** | **worldofwarcraft** | **ssdp** |
| **bgp** | **ident** | **rlogin** | **x11** | **ssh** |
| **biff** | **imap** | **rtsp** | **xboxlive** | **ssl** |
| **bittorrent** | **ipp** | **shoutcast** | **xunleinapster** | **subspace** |
| **ciscovpn** | **irc** | **sip** | **nbns** | **teamspeak** |
| **citrix** | **jabber** | **skypeout** | **ncp** | **telnet** |
| **counterstrike-source** | **kugoo** | **skypetoskype** | **netbios** | **tesla** |
| **cvs** | **l7** | **smb** | **nntp** | **tftp** |
| **dayofdefeat-source** | **live365** | **smtp** | **ntp** | **thecircle** |
| **dhcp** | **lpd** | **snmp** | **openft** | **tls** |
| **directconnect** | **msn-filetransfer** | **socks** | **pcanywhere** | **tsp** |
| **dns** | **msnmessenger** | **soribada** | **poco** | **unknown** |
| **doom3** | **mute** | **soulseek** | **pop3** | **uucp** |
| **edonkey** | **yahoo** | **ssdp** | **pressplay** | **validcertssl** |
| **fasttrack** | **zmaap** | **ssh** | **qq** | **ventrilo** |
| **finger** | **napster** | **ssl** | **quake1** | **vnc** |
| **freenet** | **nbns** | **subspace** | **quake-halflife** | **whois** |
| **ftp** | **ncp** | **teamspeak** | **rdp** | **worldofwarcraft** |
| **gkrellm** | **netbios** | **telnet** | **rlogin** | **x11** |
| **gnucleuslan** | **nntp** | **tesla** | **rtsp** | **xboxlive** |
| **gnutella** | **ntp** | **tftp** | **shoutcast** | **xunlei** |
| **goboogy** | **openft** | **thecircle** | **sip** | |
| | **pcanywhere** | **tls** | **skypeout** | |
| | | **tsp** | **skypetoskype** | |

## 6.2 Port Filter

Enables and configures the port filtering, for the blocking of specific TCP and/or UDP ports.

### 6.3 Port Forwarding

Enables and configures the port forwarding, allowing for internet incoming traffic on specific TCP and/or UDP ports to be forwarded to defined IPs in the internal network.

### 6.4 IP Filter

Enables and configures the IP filtering, for the blocking of specific IP addresses.

### 6.5 MAC Filter

Enables and configures the MAC filtering, for the blocking of specific MAC addresses.

### 6.6 DMZ Zone

Configures one host in the internal network to be "exposed" to the internet. No blocking or filtering is active for this host.

# 7. Bandwidth Control

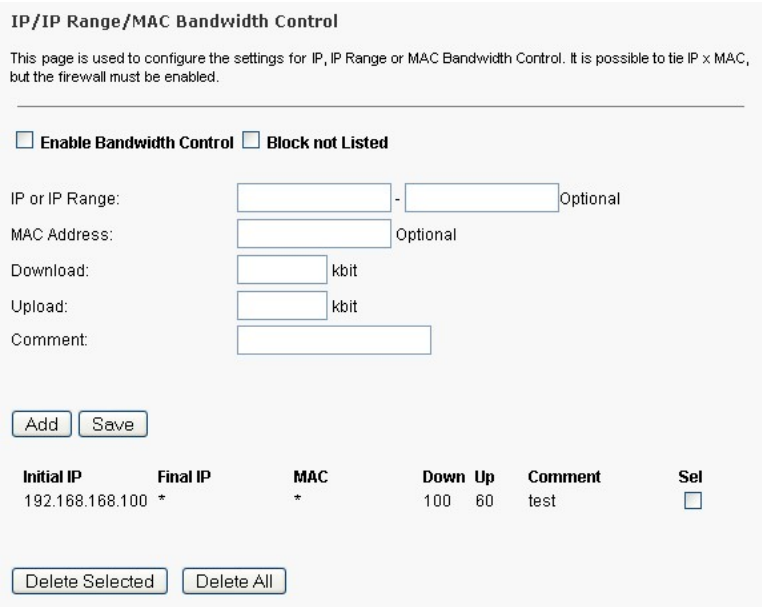
## 7.1 Interface Bandwidth

Configures the bandwidth control, for uploads and downloads to/from the internet.

## 7.2 IP/MAC Bandwidth

### 7.2.1 IP/IP Range/MAC Bandwidth Control

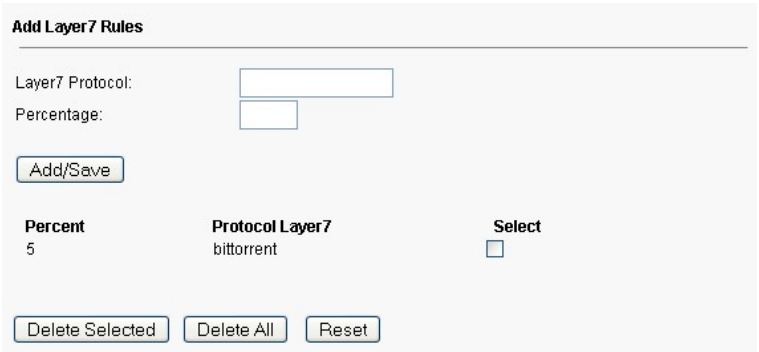
Configures bandwidth control by setting up individual up/download limits for each IP range, MAC or IP address.




With the **Block not Listed** option set, IPs, MACs, or combinations of IP+MAC not in the list will be blocked.

### 7.2.2 Add Layer7 Rules

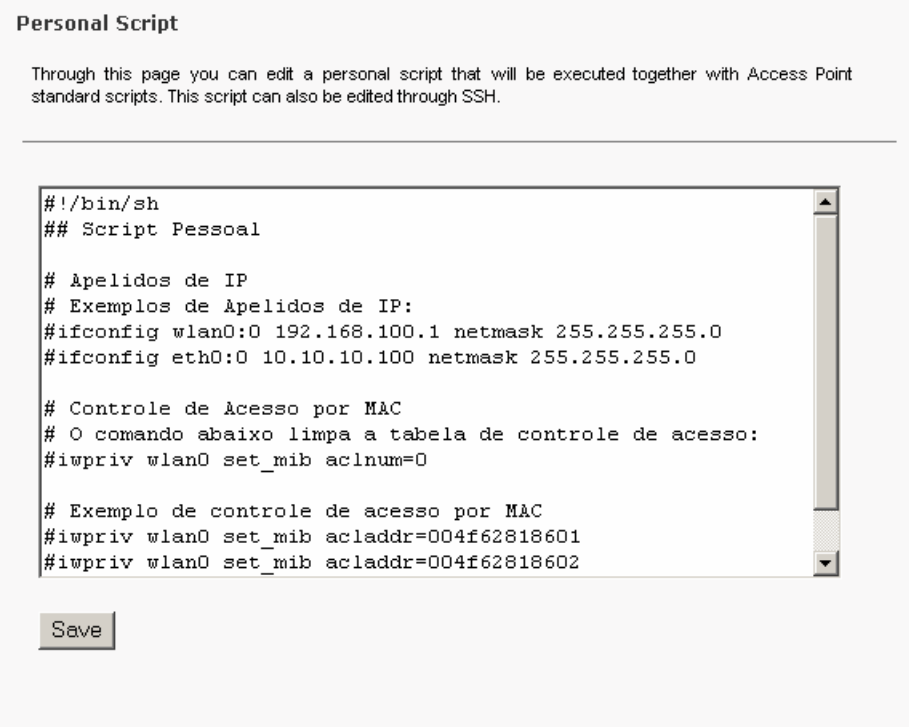
Configures the maximum percentage of the total bandwidth which can be used by a specific protocol. In the setting below, if all clients are concurrently using bittorrent to transfer files, the bandwidth usage will be limited to 5% of the total bandwidth.



# 8. Others

## 8.1 Personal script

The personal script is a shell script which is ran in the device's initialization phase. It can be used to set up IP aliasing, access control by MAC, or any other configuration accessible through the command line.


Personal Script
Through this page you can edit a personal script that will be executed together with Access Point standard scripts. This script can also be edited through SSH.
#!/bin/sh
## Script Pessoal
# Apelidos de IP
# Exemplos de Apelidos de IP:
#ifconfig wlan0:0 192.168.100.1 netmask 255.255.255.0
#ifconfig eth0:0 10.10.10.100 netmask 255.255.255.0
# Controle de Acesso por MAC
# O comando abaixo limpa a tabela de controle de acesso:
#iwpriv wlan0 set_mib aclnum=0
# Exemplo de controle de acesso por MAC
#iwpriv wlan0 set_mib acladdr=004f62818601
#iwpriv wlan0 set_mib acladdr=004f62818602
Save

## 8.2 Ethers/DHCP script

Edits the IP/MAC address table, to be used both to tie IPs to specific MAC addresses, and for the static DHCP. That is going to block MACs which don't match the specified IP address, and fix the values or the DHCP.

## 8.3 Proxy ARP script

Edits the Proxy ARP script, which enables and configures this function in the router.

## 8.4 Reboot

Reboots the device.

## 8.5 System Commands

Execute commands in the device's shell, and returns the result.

## 8.6 Date/Time

Sets the device Date and Time, and optionally configures it to be a NTP client.

## 8.7 Upgrade Firmware

Uploads a firmware file to the device.

## 8.8 Save Configurations

Saves/Restores the device configuration to/from a file in your computer. It is also possible to reset the device to the default settings.

## 8.9 License

Uploads a license file to the device – required for OLSR use (units purchased from Solwise already have the license loaded for OLSR).

### 8.10 Password

Creates/Sets a user and password for accessing the web interface.

### 8.11 Watchdog

Enables the watchdog function; the device will ping a configured IP address periodically, and if there is no answer, it will reboot.

### 8.12 Dynamic DNS

Configures the device to update its IP address in a Dynamic DNS service provider. Useful for dynamically assigned IPs.

### 8.13 Apply Configurations

Applies all the saved configurations, and reboots the device.